Office of the Governor
State Chief Information Officer

SECURITY

Chapter 1 – Classifying Information and Data

Scope: These standards apply to all public agencies, their agents or designees subject to N.C.G.S. Article 3D of Chapter 147, "State Information Technology Services."

Statutory Authority: N.C.G.S. 147-33.110

Section 01 Setting Classification Standards

010101 Defining Information

Purpose: To protect the State's information.

STANDARD

Information includes all data, regardless of physical form or characteristics, made or received in connection with the transaction of public business by any agency of State government.

The State's information shall be handled in a manner that protects the information from unauthorized or accidental disclosure, modification or loss. All agencies shall maintain a comprehensive and up-to-date database of their information assets and periodically review the database to ensure that it is complete and accurate.

ISO 17799: 2005 REFERENCE
7.2.1 Classification guidelines

010102 Labeling Classified Information

Purpose: To protect the State's Information through proper classification.

STANDARD

All data shall be labeled to reflect their classification, including their confidentiality, criticality and value to the agency and the public. All data must be clearly labeled so that all users are aware of the custodian, classification and value of the data.

RELATED INFORMATION
Standard 030302 Using and Receiving Digital Signatures
Standard 030501 Transferring and Exchanging Data

ISO 17799: 2005 REFERENCE
7.2.2 Information labeling and handling

010103 Storing and Handling Classified Information

Purpose: To protect the State's Information through the establishment of proper controls.

STANDARD

The State's information, data and documents shall be handled in a manner that will protect the information, data and documents from unauthorized or accidental disclosure, modification or loss. All information, data and documents must be processed and stored in accordance with the classification levels assigned to those data in order to protect their integrity, availability and, if applicable, confidentiality.

The type and degree of protection required shall be commensurate with the nature of the information, the operating environment, and the potential exposures resulting from loss, misuse or unauthorized access to or modification of the data.

An agency that uses confidential information from another agency shall observe and maintain the confidentiality conditions imposed by the providing agency.

Special protection and handling shall be provided for information that is covered by statutes that address, for example, the confidentiality of financial records, taxpayer information and individual census data.

GUIDELINES

- An appropriate set of procedures should be defined for information labelling and handling in accordance with the classification scheme adopted by the agency. The procedures should cover information assets in both physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information-processing activity:
  - Copying
  - Storage
  - Transmission by post, fax, and electronic mail
  - Transmission by spoken word, including mobile phone, voice mail, and answering machines
- Output from systems containing information that is classified as confidential or critical should carry an appropriate classification label. The labelling should reflect the classification according to the rules established by Standard 010102, Setting Classification Standards—Labelling Information. Items for consideration include printed reports, screen displays, recorded media (e.g., tapes, disks, CDs, cassettes, USB flash memory drives), electronic messages and file transfers.

- Where appropriate, physical assets should be labelled. Physical labels are generally the most appropriate forms of labelling. However, some information assets, such as documents in electronic form, cannot be physically labelled and electronic means of labelling need to be used. In other cases, such as with tapes, a physical label is appropriate for the outside of the tape in addition to electronic labelling of documents contained on the tape.
- The originator of a telephone call, a telex/cable, a facsimile transmission, an email, a computer transaction, or any other telecommunications transmission should be aware of the possibility of compromise of confidentiality or integrity of the information transmitted and determine whether the information requires additional special protection and handling.

RELATED INFORMATION
Standard 010107 Setting Classification Standards—Managing Network Security

ISO 17799: 2005 REFERENCE
10.7.3 Information handling procedures

010104 Isolating Top Secret Information

Purpose: To protect classified federal information.

STANDARD

When agencies receive information, data or documents classified as Top Secret from the federal government, that information, those data, or those documents shall be stored in a separate secure area and handled as required by federal law.

ISO 17799: 2005 REFERENCES
7.2.2 Information labeling and handling
11.6.2 Sensitive system isolation

010105 Classifying Information

Purpose: To protect the State's information.

STANDARD

All agency information and data shall be classified as to its confidentiality, its value and its criticality. Agencies shall establish procedures for evaluating information and data to ensure that they are classified appropriately.

Confidentiality is to be determined in accordance with N.C.G.S. Chapter 132—Public Records Law—and all other applicable legal and regulatory requirements. Data, files, and software shall be marked with a designator that identifies the process by which such information is to be made available or accessible.

ISO 17799: 2005 REFERENCE
7.2 Information classification

010106 Accepting Ownership for Classified Information

Purpose: To establish procedures for data handling

STANDARD

Agency custodians of data and their designees are responsible for agency data and shall establish procedures for appropriate data handling.

RELATED INFORMATION

Standard 010103 Setting Classification Standards—Storing and Handling Information

ISO 17799: 2005 REFERENCES
7.1.1 Inventory of assets
7.1.2 Ownership of assets
7.2 Information classification

010107 Managing Network Security

Purpose: To protect the State's information through access control procedures.

STANDARD

Network security shall be managed by each agency based on business needs and the associated risks.

Access to information available through the State network shall be strictly controlled in accordance with approved access control procedures. Users shall have direct access only to those services that they have been authorized to use.

ISO 17799: 2005 REFERENCE
10.6.1 Network controls

HISTORY

Approved by State CIO: November 18, 2005
Original Issue Date: November 18, 2005
Subsequent History:

Standard Number	Version	Date	Change/Description (Table Headings)

Old Security Policy/Standard	New Standard Numbers
Information Asset Protection	010101 – Defining Information
	010103 – Storing and Handling Classified Information
	020121 – Acceptable Usage of Information Assets
Policy and Guidelines for Handling Data	010103 – Storing and Handling Classified Information

	010104 – Isolating Top Secret Information
	010105 – Classifying Information
	010106 – Accepting Ownership for Classified Information